~~S-E-C-R-E-T~~

IBSEC-CSS-M-18
27 January 1970

COMPUTER SECURITY SUBCOMMITTEE

OF THE

UNITED STATES INTELLIGENCE BOARD

SECURITY COMMITTEE

Minutes of Meeting
Held at CIA Headquarters
Langley, Virginia
27 January 1970

1. The eighteenth meeting of the Computer Security Subcommittee was held on 27 January 1970 between 1330 and 1600 hours in Room 4E-64, CIA Headquarters. In attendance were:

[redacted] STAT
Mr. Richard F. Kitterman, State Member
[redacted] STAT
Mr. Thomas A Eccleston, Army Member
Mr. Robert B. Cameron, Navy Member
Mr. William S. Donaldson, Air Force Alternate
[redacted] STAT
Mr. Raymond J. Brady, AEC Member
Mr. Donald R. Roderick, FBI Member
[redacted] STAT
Mr. Alexander S. Chodakowski, State
[redacted] STAT
Mr. Conrad S. Banner, FBI

2. The security level of the meeting was announced as Top Secret COMINT.

Group 1
Excluded from automatic
downgrading and
declassification

~~S-E-C-R-E-T~~

3. Approval of Minutes: The minutes of the 13 January 1970 meeting were approved without amendment.

4. Security Labeling Standards: The Chairman reported that a meeting had been held on 20 January of those involved in the security labeling standards project. Copies of the Task Team's report of this meeting, prepared by [redacted] were distributed to members. The results of the 20 January meeting reflected agreement to defer decision of the question raised by DIA as to whether illegal security and dissemination "flags" should be included in the Subcommittee's product of this effort. In the collection phase of the project, a necessity was recognized for including all classification and dissemination caveats utilized in the Community with the exception of those limited to use within an individual agency. The Task Team's meeting also reflected an approach to the collection and compilation task. STAT

5. The Chairman outlined this approach in requesting all Subcommittee members to compile a listing of dissemination controls and distribution indicators utilized within their separate organizations. It was suggested that the Service representatives coordinate their submissions with the DIA member.

6. It was agreed that the NSA member would compile and provide the dissemination indicators utilized for COMINT, sensitive SIGINT, and cryptographic material. The Chairman will input the control caveats utilized for TK and B material. The AEC member was requested to furnish those applying to Restricted Data and other AEC controlled material.

7. In discussion that followed the Chairman suggested that each agency submission not only list the caveats but also briefly identify their meaning. Concerning specially controlled material, the caveats should be annotated with reference to their classification. Included in the listings would be any dissemination indicators or special control systems not previously discussed at the Task Team or Subcommittee level, including special indicators for SEATO, NATO, etc.

8. In developing agency submissions, the following guidelines were provided:

A. Exclude indicators peculiar to a single agency, as material bearing such indicators is not disseminated outside of that agency;

B. Include a brief definition for each indicator;

C. Show what "clearances" are required for access to material bearing each caveat;

D. Include synonyms used for indicators, where applicable;

E. Emphasize that the Subcommittee is not studying the problem of illegal caveats, but merely attempting to develop standards for the translation of security "flags" used in the Community.

Members were requested to submit their replies on this project to the Chairman on or before 24 February.

9. Incidental to the above discussion, members were furnished a copy of IBSEC-PR/45 dated 16 January 1970, a joint memorandum for all Security Committee and IHC members outlining the approach being taken with reference to the problem of standards for security classification and dissemination control indicators in Community data bases.

10. Training Course Task Team: Mr. Cameron reported that this Task Team had not met since the previous Computer Security Subcommittee meeting; he advised that a meeting was planned before 6 February. The Army clarified the earlier report from the Army Security Committee member with reference to Army participation in a DoD Computer Security Course. Mr. Eccleston indicated that the Department of Army is not participating in the development of such a course, but along with other Service representatives had been solicited for comments concerning the security training requirements involved in the implementation of the National Military Command Center. No duplication of effort with Computer Security Subcommittee plans to develop a computer security training course is indicated.

11. Multilevel Operations: The Chairman again reminded the Army and Navy members that he had not yet received their submissions for the proposed Subcommittee consolidated report on key protection features useable in multilevel systems. The Navy representative submitted an interim response at the instant meeting indicating that a survey of Naval commands is in process, but not yet completed with respect to this project.

12. The Chairman also reported that he had been invited to a meeting scheduled for 11 February of the COINS Software Security Panel which was scheduled to discuss a proposal for addressing the "need-to-know" problem in the operation of that network.

13. To permit the basis for later discussion, during the instant meeting the Chairman presented some thoughts concerning basic requirements for the operation of a multilevel computer system. He opened these remarks with the personal comment that there appeared to be hope for permitting the operation of a time sharing computer system in a multilevel security environment provided that this environment was "benign". In this context, a "benign" environment was defined as one where all personnel having access to the time sharing system would hold Top Secret security clearances, and the compartmentation problem for the multilevel operation was limited to one of compartmentation of specially controlled groups of data. A classic example of such an operation would be a system storing and processing collateral and compartmented intelligence data in which all personnel would hold Top Secret clearances, but not all would have access approvals for the compartmented material.

14. Recognizing the problem as one of compartmentation, the Chairman expressed his thinking that a few basic security factors built into the operation of such a system might suffice to provide an adequate assurance that compartmentation could be controlled by the system itself. For discussion purposes, he proposed four basic tools for controlling this compartmentation:

A. A software based user identification and authentication routine, in which each user would have a unique authentication code, and by which a user would be identified as being authorized for general or limited system access and his identity authenticated;

B. Keyword protection of files by which a capability would exist to limit access to designated files to those persons knowing a specific password, which would be changed periodically;

C. Basic physical security and access control procedures to protect the computer center itself and its remotely located terminals as well as interconnecting links;

D. A working audit trail capability which would generate a system log of all queries to the system, identifying the user, the terminal involved, the time, the files accessed, any incorrect or invalid query attempts, etc.; this log would have to be reviewed regularly both by the individual assigned the responsibility for system security and by (in part) the monitor of each terminal location, as a check to insure against unauthorized terminal access.

15. The Chairman emphasized that the four features outlined above were not meant to be comprehensive but rather basic requirements under which a given system could be approved to operate at different security levels in a "benign" environment. Discussion that followed recognized additional features, some of which might be considered as mandatory for multilevel operations, including read and/or write protection, automatic log off procedures, etc.

16. No prolonged discussion on this topic was had at the instant meeting. Nevertheless members were requested to give thought both to the problem and to the specific concepts outlined, since the Subcommittee will be addressing the overall multilevel problem in considerable detail in the months ahead.

17. Computer Security Threat Analysis: The Chairman referenced the discussion at the 19 January 1970 Security Committee meeting predicated on the request of the Army member that it would be appropriate to analyze and evaluate the threat posed by the vulnerabilities of Community computer operations. The Security Committee discussion of this issue reflected agreement that the CI Staff of CIA be tasked to report any known cases where opposition Services had attempted to exploit the vulnerabilities of computer operations for intelligence purposes; in addition the Subcommittee was tasked to study and report on the postulated threat in the computer environment.

18. The Subcommittee Army member clarified the earlier request presented to the Security Committee, indicating the Army's desire to limit this threat analysis to the CI Staff action noted above. Subcommittee members unanimously agreed that a study of the postulated threat posed by the Community's use of modern computing equipment was superfluous, since this threat is already well defined and recognized both in the Security Community, the ADP technical environment, and by the President's Foreign Intelligence Advisory Board.

19. The Chairman announced that he had already initiated action requesting information on known computer espionage cases from the CI Staff of CIA. Members were requested to solicit the same type of information from appropriate components of their own organizations and to submit reports to the Chairman on or before the 9 February Subcommittee meeting. It is anticipated that a consolidated report will be prepared for submission to the Security Committee at its 16 February meeting.

20. Other Business:

A. Security Evaluation of Community Systems: The Chairman introduced the necessity for the Subcommittee's eventual consideration of the problem of evaluating the security protection features of modern computer systems. He outlined the need

for system evaluation in quantitative terms as a basis for system security certification. Such evaluation addresses the effectiveness of security features in the hardware, software, and basic physical and procedural security aspects of system operations. As an introduction to this topic, the Chairman announced his plan to have a representative of CIA's Office of Research and Development brief the Subcommittee at a future meeting on a recently completed contract to assess the security of the hardware of a specific IBM system;

B. Change in Meeting Time: At the request of the NSA and AEC members and with the unanimous agreement of the Subcommittee, the time of future Subcommittee meetings was changed to Mondays at 0930 hours.

21. The next Subcommittee meeting was scheduled for 0930 hours on 9 February 1970.

STAT

Chairman
Computer Security Subcommittee